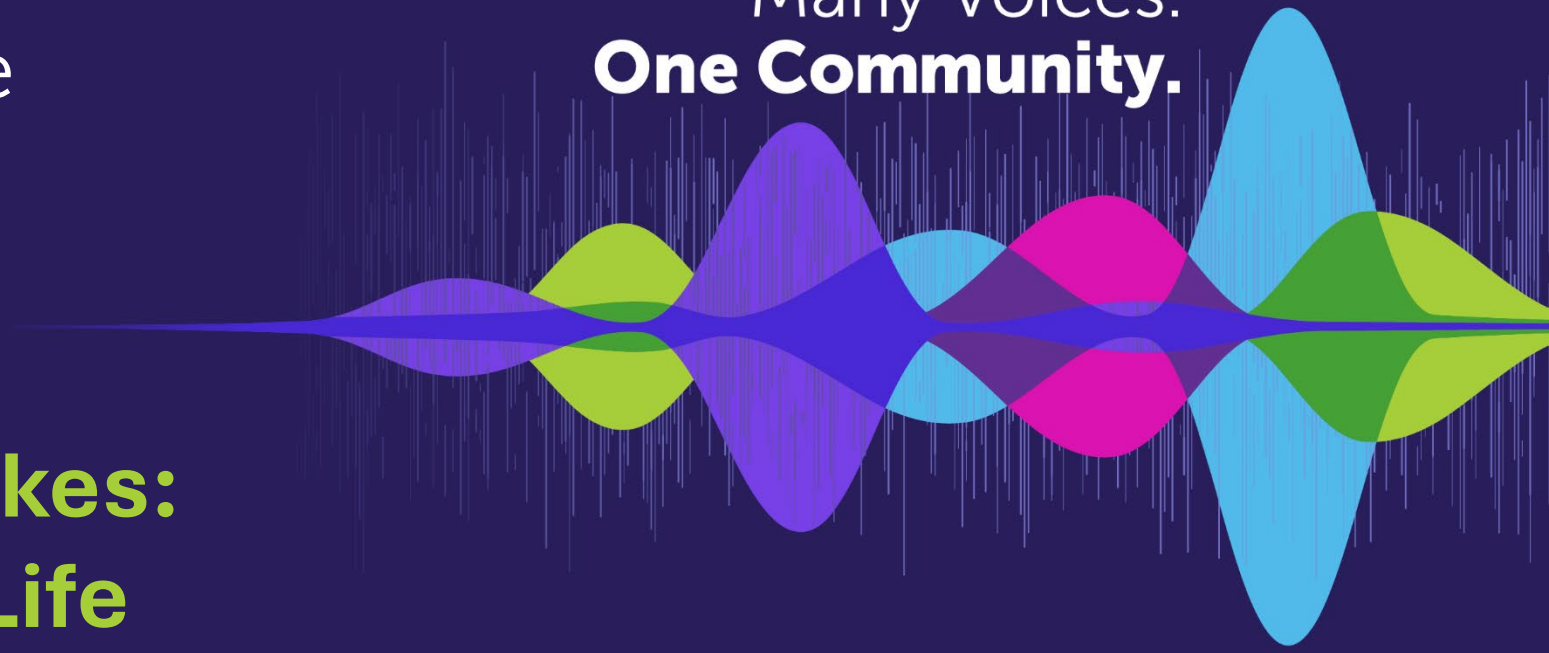
RSAC 2025 Conference

Many Voices.
One Community.

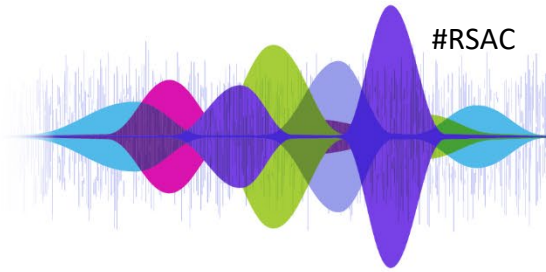


SESSION ID: PHF-M05

Home Tech, High Stakes: Securing the Digital Life

Jennifer (JJ) Minella

Principal Security Advisor
Viszen Security and CISO Launch®
https://www.linkedin.com/in/jenniferminella/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Products mentioned in this presentation are not endorsements.

Specific brands and product models are shown for context and to assist in researching solutions.

Jennifer (JJ) Minella

AUTHOR | SPEAKER | ADVISOR

Meet Jennifer (JJ) Minella

- 20+ years in technology, 15+ years in security
- SC Magazine Top 10 Power Players
- Member Forbes Technology Council
- CSA Zero Trust Working Group leadership
- Specialties in network and wireless architecture and security
- IoT security, OT-IT security
- Faculty with IANS Research
- Former (ISC)2 International board of directors and chairperson
- Author of *Wireless Security Architecture* and *Low Tech Hacking*
- Award winning blog at https://securityuncorked.com
- Founder and principal advisor Viszen Security
- Volunteer with RSAC, EWF, BSides, CyberPatriot and others
- **@jjx** on Social Media (Twitter, Bluesky, Mastodon)

2023 OFFICIAL MEMBER Forbes Technology Council

Follow Me for More

Follow me on LinkedIn for articles, live events, free resources, and training

Viszen Security

IANS

Packet Protector

The Podcast at the Intersection of Networking and Security

Meet the 3 Home Tech Personas

"I just want my Netflix to work."

The Low-Tech Lifer

"I tinker, I configure, I am the master of my domain." =(^.^)=

The DIY Home Admin

"My risk is higher, and so is my defense."

The Hardened Defender

The Low-Tech Lifer

Assumptions and Environment

- Uses ISP-provided modem/router (CPE)
- No major configuration beyond the default setup
- Prioritizes simplicity over security
- Needs clear, low-effort wins to reduce risk
- Receives the basic ‘friends and family’ recommendations

"I tinker, I configure, I am the master of my domain." =(^.^)=

The DIY Home Admin

Assumptions and Environment

- Uses SOHO equipment like retail Wi-Fi routers
- Has managed switches that support VLANs
- Comfortable with web GUIs and setup screens
- Understands DNS and basic network services
- Wants smart, manageable upgrades to boost home network security
- More tech savvy and capable than the average bear, but not ready to turn home networking into a full-time job

The Hardened Defender

Assumptions and Environment

- Executive, public figure, or otherwise targeted user
- Can fund an enterprise-grade network stack
- Potentially has home network managed or monitored by corporation or 3rd party
- Likely has IoT connected home security systems
- Environment will use extensive segmentation, 802.1X, MFA, and enterprise best practices
- Needs controls that match corporate-level threat models

Home Tech Security in [illegible]

ADVOCACY

Mozilla Publishes Ring Doorbell Vulnerability Following Amazon's Apathy

By **Mozilla** | June 6, 2023

Mozilla disclosure comes mere days after Ring reaches $5.8 million settlement with the FTC for other privacy issues

SMART HOME • 1 min read •

Bitdefender Finds Ring Doorbell Vulnerability that Exposes User's Wi-Fi Password

Silviu STAHIE
November 08, 2019

Promo Protect all your devices, without slowing them down.
Free 30-day trial

Home Tech Security in '...

ADVOCACY

Mozilla Publishes Ring Vulnerability Following Apathy

By **Mozilla** | June 6, 2023

Mozilla disclosure comes mere days after Ring settlement with the FTC for other privacy issue

SMART HOME • 1 min read •

Bitdefender Finds Ring Doorbell Vulnerability that Exposes User Password

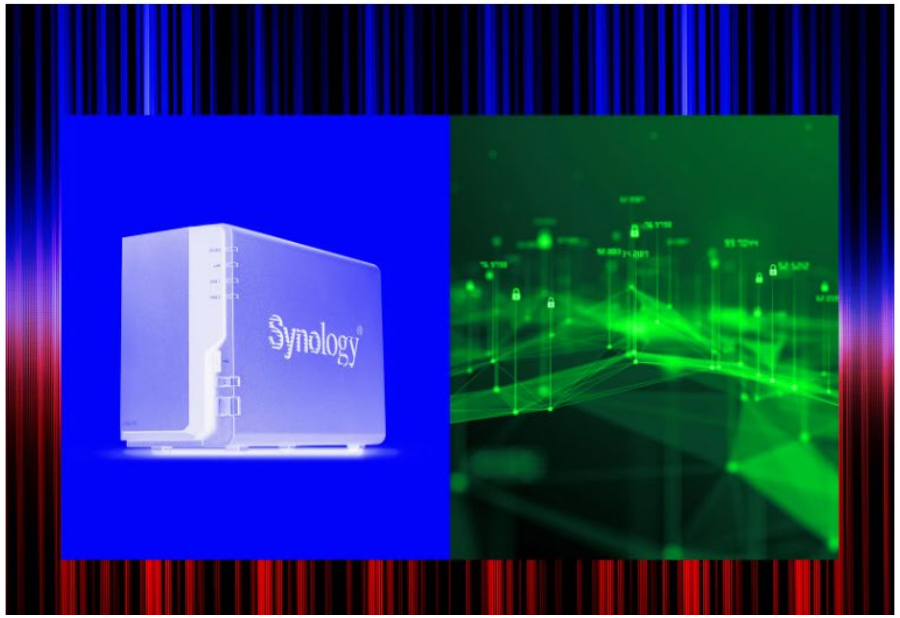
...ring them down.

WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH SIGN IN | GIVE A GIFT

KIM ZETTER SECURITY NOV 1, 2024 6:00 AM

Zero-Click Flaw Exposes Potentially Millions of Popular Storage Devices to Attack

A vulnerability categorized as "critical" in a photo app installed by default on Synology network-attached storage devices could give attackers the ability to steal data and worse.



Viszen Security

RSAC 2025 Conference

Home Tech Security in '...

ADVOCACY

Mozilla Publishes Ring Vulnerability Following Apathy

By **Mozilla** | June 6, 2023

Mozilla disclosure comes mere days after Ring settlement with the FTC for other privacy issue

SMART HOME • 1 min read •

Bitdefender Finds Ring Doorbell Vulnerability that Exposes User Password

WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH SIGN IN GIVE A GIFT

KIM ZETTER SECURITY NOV 1, 2024 6:00 AM

Zero-Click Flaw Exposes Potentially Millions of Popular Storage Devices to Attack

A vulnerability categorized as "critical" in a photo app installed by default on Synology network-attached storage devices could give attackers the ability to steal data and worse.

AUDIO/VIDEO | AV ACCESSORIES | DEVICES/EQUIPMENT | DISPLAYS | MEDIA | NETWORKING | NEWS | WIRELESS

JUNE 28, 2024

Critical Cybersecurity Vulnerabilities in Smart Home Devices Uncovered in New Research

Report from NETGEAR and cybersecurity firm Bitdefender details the most vulnerable and commonly targeted smart home devices.

Viszen Security

Home Tech Security in '...

SMART HOME • 1 min re...

Bitde...

ds Ring Doo...bell Vulnerability

...sword

...ring them down.

SIGN IN | GIVE A GIFT

...age

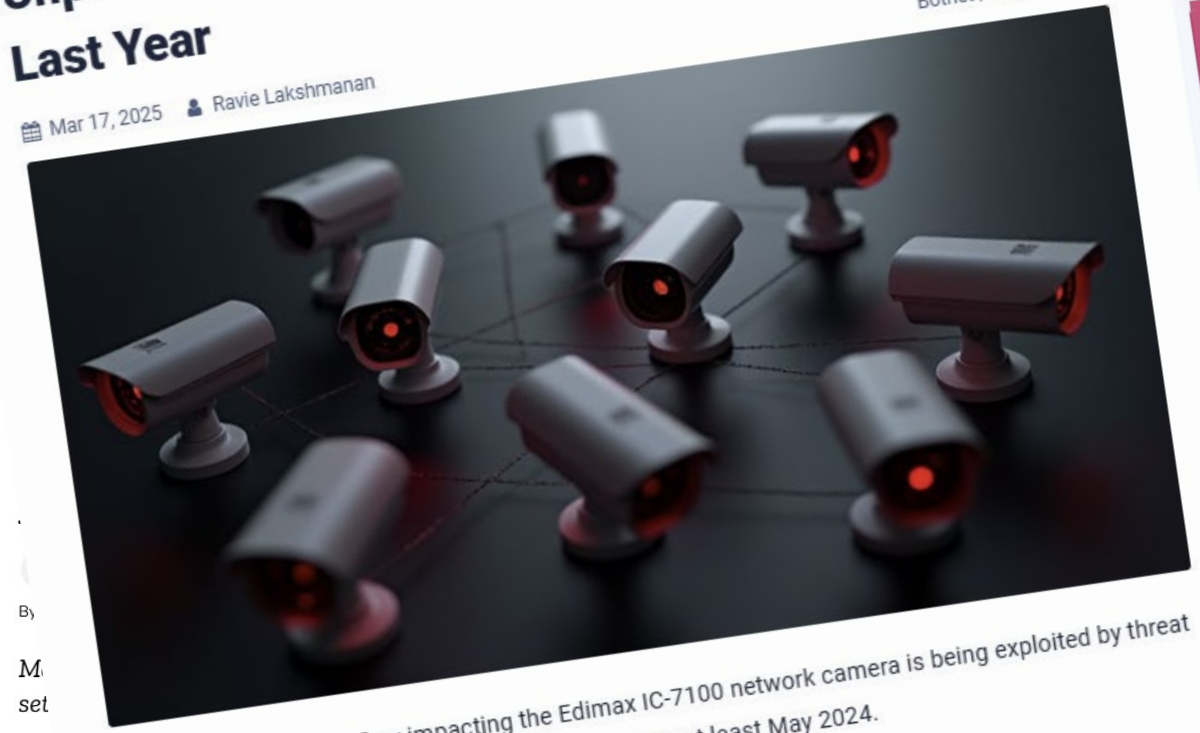
...torage devices

JUNE 28, 2024

Botnet / Vulnerability

Unpatched Edimax Camera Flaw Exploited for Mirai Botnet Attacks Since Last Year

Mar 17, 2025 Ravie Lakshmanan



An unpatched security flaw impacting the Edimax IC-7100 network camera is being exploited by threat actors to deliver **Mirat botnet malware variants** since at least May 2024.

The vulnerability in question is **CVE-2025-1316** (CVSS v4 score: 9.3), a critical operating system command injection flaw that an attacker could exploit to achieve remote code execution on susceptible devices by means of a specially crafted request.

...curity
Smart
...covered
...rch

Trending News

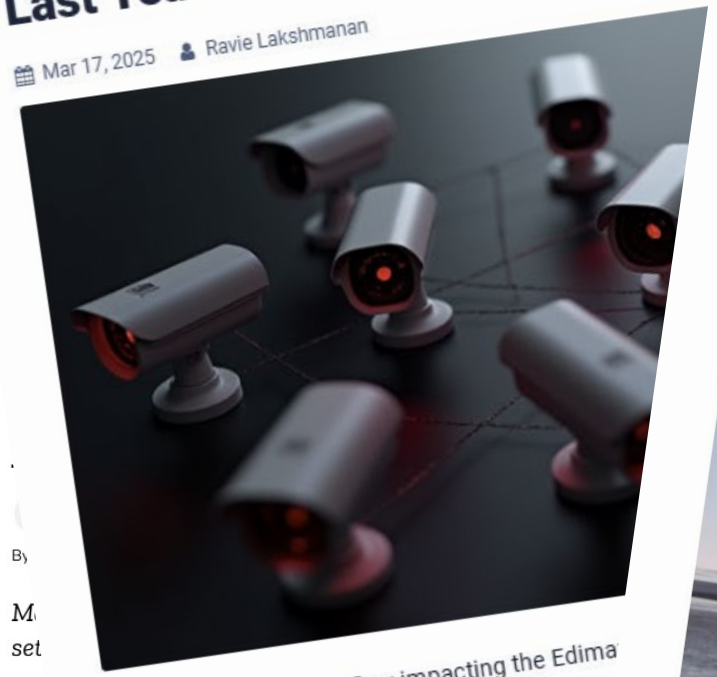
...GEAR and cybersecurity firm Bitdefender ...he most vulnerable and commonly targeted smart ...nome devices.

...ference

Home Tech Se

Unpatched Edimax Camera Flaw Ex Last Year

Mar 17, 2025 Ravie Lakshmanan



An unpatched security flaw impacting the Edima
actors to deliver Mirat botnet malware variants sinc

The vulnerability in question is CVE-2025-1316 (CVSS v4 score: 9.3), a critic
command injection flaw that an attacker could exploit to achieve remote code execution o
susceptible devices by means of a specially crafted request.

SMART HOME • 1 min re

WIRED

FEATURED SUPERHUMAN GADGETS DINOSAUR CHOIR BUY IT FOR LIFE AIRPORT THEORY THE WIRED 101 DEALS DELIVERED SIGN IN GIVE A GIFT

SIMON HILL GEAR FEB 21, 2025 8:30 AM

The US Is Considering a TP-Link Router Ban—Should You Worry?

Several government departments are investigating TP-Link routers over Chinese cyberattack fears, but the company denies links.

nome devices.

vulnerable and commonly targeted smart

Bitdefender

ference

Home Tech Se

CYBERSECURITY DIVE

Deep Dive Library Events Press Releases

Strategy Breaches Vulnerability Cyberattacks Threats Leadership & Careers Po

Emerging botnet exploits TP-Link router flaw posing risk to US organizations

Ballista's attacks on TP-Link devices comes as U.S. lawmakers consider banning the company's products over suspected links to China.

Published March 12, 2025

By Elizabeth Montalbano, Contributing Reporter

SMART HOME • 1 min re

WIRED

R CHOIR BUY IT FOR LIFE AIRPORT THEORY THE WIRED 181 DEALS DELIVERED SIGN IN GIVE A GIFT

ink Router Ban—Should You Worry?

-Link routers over Chinese cyberattack fears, but the company denies

inerable and commonly targeted smart

ference

Devices in your home (and office) routing unauthorized traffic

Graphic Source: RunZero Research Report

Three Home Tech Domains That Matter

Home Networking and Wi-Fi

IoT and Connected Things

Personal VPNs

RSAC 2025 Conference

"I just want my Netflix to work."

The Low-Tech Lifer

Basic Home Tech Hygiene

The Low-Tech Lifer Setup

Internet Router
and Wi-Fi from ISP

A few wired ports on
the CPE hardware

Laptops, phones,
and tablets

Most devices are
Wi-Fi connected

Some IoT, streaming devices,
and smart home tech

Recommended for the Low-Tech Lifer

Home Networking and Wi-Fi

- No Hidden SSIDs
  - Hiding SSIDs offers 0 security. It's OK (but not recommended) to hide (for convenience) SSIDs serving endpoints that don't leave the house
- Separate guest networks
  - Use ISP CPE built in functions (guest NAT, segmentation, multi SSID)
- Use WPA3 security where possible
  - Especially for passphrase networks
- Create separate WPA2 and WPA3 networks for passphrases
- Change default passwords to CPE/router/Wi-Fi management
- Change default passwords to passphrase SSIDs
- Update firmware!

Recommended for the Low-Tech Lifer

IoT and Connected Things

Printers

- Configure management and remove default passwords
- Run software updates regularly (both on-printer and on computers)

Home Storage

- Ensure no direct Internet connection if possible
- Configure management and remove default passwords
- Run software updates regularly
- Configure MFA for management if cloud-connected or remotely accessible

Smart Home and TVs

- Beware of privacy risks (add updated Samsung and LG privacy statements showing how they will share your detailed viewing habits with third parties for marketing)
- How to address on TVs– if using Apple TV, Amazon Fire, etc. – disable Wi-Fi on the TV itself but allow the streaming device Internet access
- How to address on other devices – carefully review policy and determine if the risk is acceptable or not and if Internet is required or not
- Be aware of pivot points and network adjacency
- For home security IoT (cameras, locks, etc.) always use MFA for management and sign up to receive the manufacturer's alerts and updates

Recommended for the Low-Tech Lifer

Personal VPNs

Remember use cases for VPNs – Do you care, and when?

- Connectivity to remote resource
- Privacy to obscure your traffic → our focus is this conversation

Use built-in personal VPNs

- Many platforms, especially smartphones have built-in VPNs

If traveling, consider VPN app

- Pay for a reputable VPN app! If it's free, YOU are the product.

Product Suggestions for the Low-Tech Lifer

Firewalls

- Most likely using the ISP CPE equipment

Switches

- Most likely using the ISP CPE equipment

Wi-Fi APs

- Most likely using the ISP CPE equipment
- Possibly residential retail with extenders or mesh (e.g., Netgear, Amazon Eero)

Storage

- WD My Cloud Home
- TP-Link Tapo *

Smart Home

- Ideally purchase a reputable brand with strong privacy protection
- Look for IoT devices that are certified for Matter protocol

VPNs

- Apple Privacy Relay
- Google One VPN
- Reputable paid apps - Protus VPN, NordVPN, IVPN

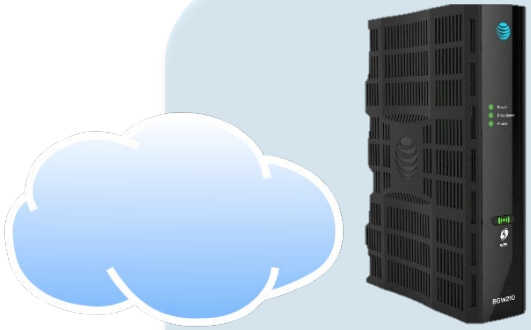
RSAC 2025 Conference

"I tinker, I configure, I am the master of my domain." =(^.^)=

The DIY Home Admin

Mid-level security for the tech-savvy homeowner

The DIY Home Admin Setup



Internet Router or raw fiber handoff from ISP

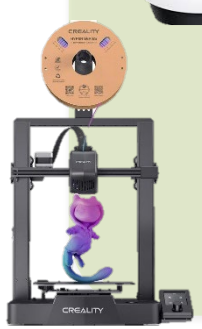
Firewall, SOHO or open source

Managed switch(es) and retail Wi-Fi APs

Both wired and Wi-Fi in home

Laptops, phones, and tablets

Much IoT, streaming devices, and smart home tech, plus home security IoT and automation



IFTTT

Recommended for the DIY Home Admin

Home Networking and Wi-Fi

- **All of the above, especially these, plus …**
  - Use WPA3 where possible
  - Create separate WPA2 and WPA3 networks for passphrases
- **Use PPSK if supported**
  - to track usage (not likely in ISP CPE equipment)
- **Change default DNS to a secure DNS solution**
  - NextDNS, Cloudflare, etc. [[examples]]
- **Manage your firewall and configure filtering**
  - OpenSense, Ubiquiti, PFsense, Microtik [[examples]]
- **Segment!**
  - (VLANs on wired side to switch or firewall; peer isolation over the air; and other Wi-Fi policies as needed e.g. VXLAN or Roles)
- **Disable risky protocols like UPnP**
- **Check the manufacturer**
  - Let’s talk about TP-Link, possible government ban (and all the TP-Link brands, e.g., Kasa Smart, Omada networking)

Recommended for the DIY Home Admin

IoT and Connected Things

Printers

- Everything above, plus…
- Disable WPS and direct Wi-Fi printing

Home Storage

- Everything above, plus…
- Filter or control access to storage and critical devices via firewall
- Configure MFA for all access if supported

Smart Home and TVs

- Everything above, plus…
- Configure VLANs or filtering to segment IoT and smart home devices from work systems and security IoT (cameras, door locks)

Recommended for the DIY Home Admin

Personal VPNs

Use built-in personal VPNs

- Many platforms, especially smartphones have built-in VPNs

Firewall-enabled VPN

- Pay for a reputable VPN app! If it's free, YOU are the product.

Overlay VPN solutions

- For the uber-security conscious DIY'er
- Look for solutions with WireGuard (preferred) or configure OpenVPN appropriately

Product Suggestions for the DIY Home Admin

Firewalls

- OPNsense (open source, free software but small learning curve)
- pfSense (open source, free software steeper learning curve)
- MicroTik firewall
- Ubiquiti firewall
- Meraki MX firewall
- Fortinet FortiGate 40 firewall
- SonicWALL TZ series firewall

Switches

- TP-Link switches *
- Netgear switches
- Ubiquiti switches
- Meraki MS switches
- Aruba InstantOn switches
- Hand-me-down Cisco, HPE, Juniper, etc. switches (ensure security updates are available)

Wi-Fi APs

- TP-Link APs *
- Netgear APs
- Ubiquiti APs
- Aruba InstantOn APs
- Meraki APs

Storage

- Synology DiskStation (Home models)
- QNAP TS series
- Asus Asustor NAS
- TerraMaster F-series
- Buffalo TeraStation SOHO

Smart Home

- Check country of origin/manufacture
- Look for strong privacy protection
- Seek and upgrade to Matter certified IoT protocol

matter

VPNs

- Paid Apps - Protus VPN, NordVPN, IVPN
- VPN via your firewall

Viszen Security

RSAC 2025 Conference

RSAC 2025 Conference

"My risk is higher, and so is my defense."

The Hardened Defender

Advanced defenses for high-value targets and the moderately paranoid

Hackers increasingly target executives' personal email & social-media accounts as initial entry points into sensitive corporate systems.

THE WALL STREET JOURNAL.
English Edition | Print Edition | Video | Audio | Latest Headlines | More
Latest World Business U.S. Politics Economy Tech Markets & Finance Opinion Arts Lifestyle Real Estate Personal Finance Health Style Sports
WSJ PRO
Cybersecurity
Home News Research Archive Newsletters Events
WSJ PRO
Public Officials Separate Workplace and Personal Online Lives. Hackers Don't Care.
Attacks on the personal accounts of VIPs are on the rise; 'They are prime targets'
By Angus Loten
April 7, 2025 3:45 pm ET | WSJ PRO
Save
Listen (1 min)
Advertisement

In a survey of 586 CISOs, **51%** identified **cyberattacks against their execs' personal accounts** last year, up from 42% in 2023.

97% of execs **access work accounts on personal** devices & **80%** send work-related emails/texts from their personal phones.

THE WALL STREET JOU

English Edition | Print Edition | Video | Audio | Latest Headlines

Latest World Business U.S. Politics Economy Tech Markets & Finance Opinion Arts Lifestyle

WSJ PRO Cybersecurity

Home News Research Archive Newsletters

WSJ PRO

Public Officials Separate Workplace and Personal Online Lives. Hackers Don't Care.

Attacks on the personal accounts of VIPs are on the rise; 'They are prime targets'

By Angus Loten

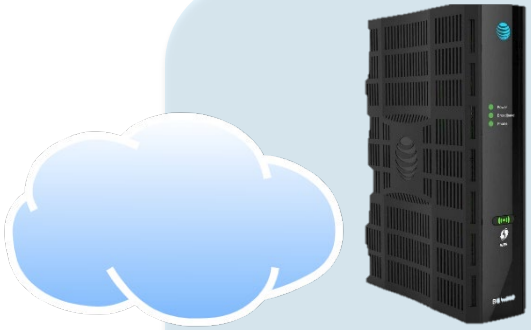
April 7, 2025 3:45 pm ET | WSJ PRO

Save Listen (1 min)

Viszen Security

RSAC 2025 Conference

The Hardened Defender Setup



Internet Router or raw fiber handoff from ISP

Enterprise branch firewall

Managed switch(es) and retail or enterprise Wi-Fi APs

Both wired and Wi-Fi in home

Personal laptops, phones, and tablets

Business laptops, phones, and tablets

Advanced home security devices

Much IoT, streaming devices, and smart home tech, plus home security IoT and automation

Environment is monitored

Recommended for the Hardened Defender

Home Networking and Wi-Fi

- **All of the above, plus…**
- **Use enterprise grade Wi-Fi products**
  - Get centralized logging and reporting
  - Advanced filtering/firewall on Wi-Fi
  - Consider products like Juniper Mist, Meraki, or Aruba InstantOn
- **Use 802.1X where possible with cloud RADIUS**
  - Consider Jump Cloud, Mist Access Assurance, Meraki Cloud NAC, etc.
- **Auto update firmware if supported**
  - Most cloud-managed network devices support this
- **Manage mDNS on network and on endpoint**
  - Filter or disallow; recommend disable for high risk/targeted execs
- **Secure management access with MFA**
  - Everything should be MFA'd at this level
- **Managed service and monitoring**
  - Have organization or partner manage when appropriate including SOC/SIEM/syslog and monitoring

Recommended for the Hardened Defender

IoT and Connected Things

Printers

- Everything above, plus…
- Logging and monitoring

Home Storage

- Everything above, plus…
- Added segmentation
- Logging and monitoring
- Tracking of vendor CVEs and KEVs

Smart Home and TVs

- Everything above, plus…
- Added segmentation (via Wi-Fi, wired, and/or firewall)
- Monitoring of traffic for anomalous behavior or unusual destinations

Recommended for the Hardened Defender

But, do we *really* care?

What can be derived from your traffic?

Personal VPNs

Hint: a LOT

Product Suggestions for the Hardened Defender

Firewalls

- Enterprise-grade, SOHO/branch sized firewall, ideally with managed service/monitoring
- Meraki MX firewall
- SonicWALL TZ series firewall
- Fortinet FortiGate 40 firewall
- Juniper SRX 300 series firewall

Switches

- Enterprise-grade, SOHO/branch sized switches
- Aruba switches
- Meraki switches
- Juniper Mist managed switches

VPNs

- Paid Apps
- VPN via your firewall
- Overlay VPN software/apps

Wi-Fi APs

- Enterprise-grade Wi-Fi, ideally with logging and alerting
- Cloud-connected and enterprise or 3rd party manage/monitor recommended
- Aruba Central managed APs
- Meraki APs
- Juniper Mist APs

Storage

- Synology Plus / XS Series
- QNAP x53D / x73A Series
- Netgear ReadyNAS
- Dell PowerEdge w/ TrueNAS (DIY)
- NetApp SolidFire Edge

Smart Home

- Check country of origin/manufacture
- Look for strong privacy protection
- Seek and upgrade to Matter certified IoT protocol

Viszen Security

RSAC 2025 Conference

How to Apply this Info…

Next Week

Make a Plan

Evaluate your home tech risks and determine which persona you are.

Next 3 Months

Start Updates

Begin executing your home tech security plan. Implement network and Wi-Fi updates. Sign up for critical product updates from vendors.

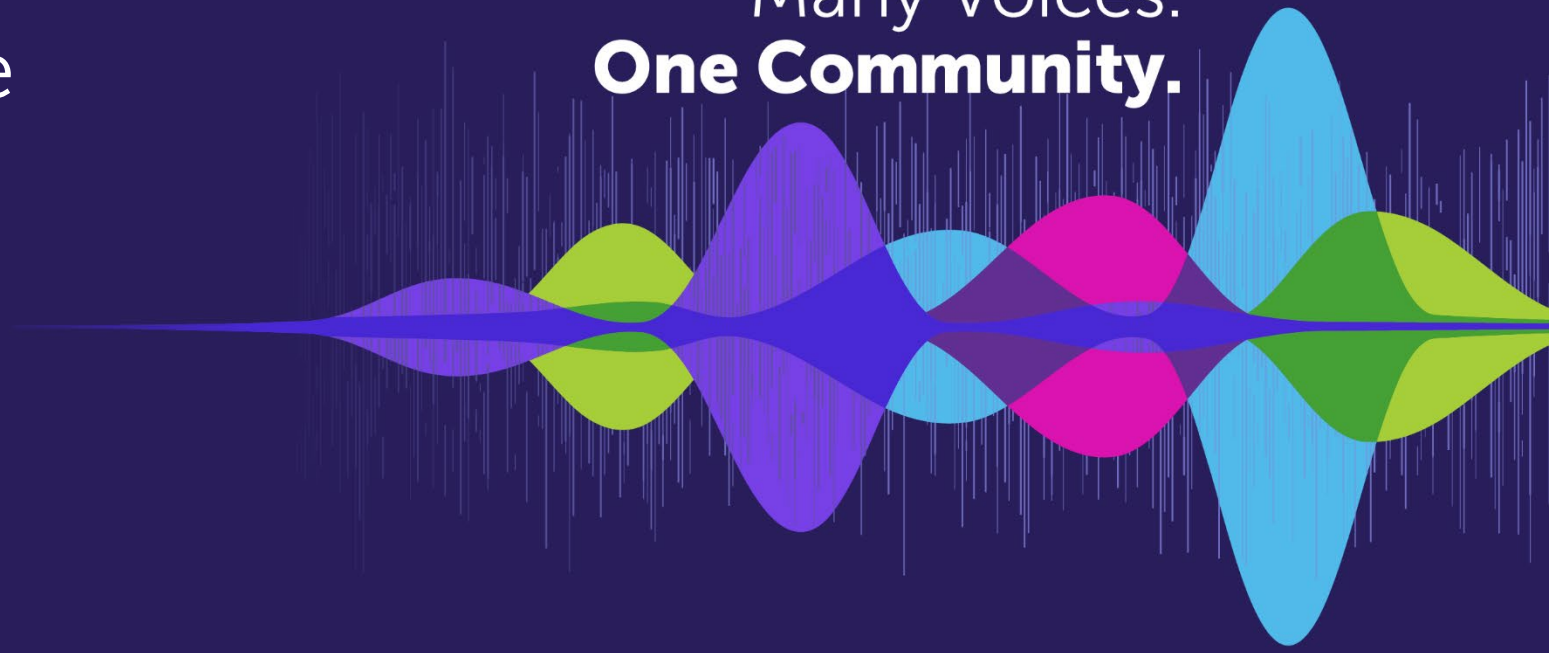
Next 6 Months

Mature Your Tech

Mature your home tech security until you've reached the proper targets for your persona.

RSAC 2025 Conference

Many Voices.
One Community.



Let’s connect!

https://www.linkedin.com/in/jenniferminella/

Viszen Security